

## UNITED STATES DISTRICT COURT

FILED

for the  
Eastern District of Missouri

JUL 24 2019

U. S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST. LOUIS

In the Matter of the Search of

THE FACEBOOK ACCOUNT ASSOCIATED WITH USER ID:  
<https://www.facebook.com/ricardo.rusanel>

Case No. 4:19-MJ-6192-PLC

## APPLICATION FOR A SEARCH WARRANT

I, Special Agent David Herr, FBI, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:  
SEE ATTACHMENT A

located in the NORTHERN District of CALIFORNIA, there is now concealed

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
18, USC, § 2113

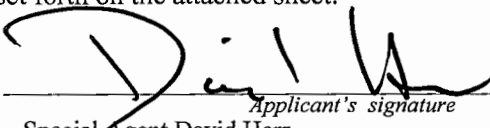
Bank Robbery

Offense Description

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
 Applicant's signature  
 Special Agent David Herr  
 Federal Bureau of Investigation (FBI)  
 Printed name and title

Sworn to before me and signed in my presence.

Date: July 24, 2019City and state: St. Louis, MO

  
 Judge's signature  
 Honorable Patricia L. Cohen, U.S. Magistrate Judge  
 Printed name and title

AUSA: EDWARD L. DOWD, III #61909MO

FILED

JUL 24 2019

U. S. DISTRICT COURT  
EASTERN DISTRICT OF MO  
ST. LOUIS

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF  
THE FACEBOOK ACCOUNT  
ASSOCIATED WITH USER ID:  
<https://www.facebook.com/ricardo.rusanel>

Case No. 4:19-MJ-6192-PLC

**Filed Under Seal**

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, David Herr, a Special Agent of the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the electronic device(s) being used to access Facebook, Inc. account <https://www.facebook.com/ricardo.rusanel> (the “Target Account”), whose service provider is **FACEBOOK, INC. (“Facebook”)**, a provider of electronic communications and/or remote computing service headquartered at **1601 Willow Road., Menlo Park, California**. The Target Account is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since 1998. I have received training at the FBI Academy in Quantico, Virginia, in criminal and national security investigative techniques. I am currently assigned to the Violent Crime Squad in the St. Louis Division and investigate violations of federal criminal law, including carjacking, bank robbery, extortion, kidnapping, interstate transportation of stolen property, and

Hobbs Act robberies. I have been the affiant and/or received training on search warrants involving these crimes.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit there is probable cause to believe that **Ricardo RUSAN** has violated **Title 18, United States Code, Section 2113**. **RUSAN** was charged with these crimes on **June 20, 2019** and is the subject of an arrest warrant issued on **June 20, 2019**. There is also probable cause to believe that the location information described in Attachment B will assist law enforcement in arresting **RUSAN**, who is a “person to be arrested” within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

5. The court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

#### **IDENTIFICATION OF THE LOCATION TO BE SEARCHED**

6. Agents and investigators request authority to search Facebook, and user accounts more fully and particularly described as:

<https://www.facebook.com/ricardo.rusanel>

Profile name: Ricardo Rusan-el

**INVESTIGATION AND PROBABLE CAUSE**

7. The United States, including **the Federal Bureau of Investigation**, is conducting a criminal investigation of **Ricardo RUSAN** regarding possible violations of **Title 18, United States Code, Section 2113**.

8. On April 16, 2019, a bank robbery occurred at the Commerce Bank, 6383 Clayton Road, Clayton, MO, in the Eastern District of Missouri. An unknown male entered the bank wearing a blue mask, dark hooded sweatshirt, dark pants and blue latex gloves and announced the robbery. The unknown male was holding a dark colored semi-automatic firearm which he pointed at employee(s). The victim teller proceeded to give the unknown male approximately \$500.00 in US Currency belonging to Commerce Bank. Surveillance video from bank confirms events and general description of suspect. Surveillance video from BP gas station, located at the corner of Clayton Road and Skinker/McCausland, revealed an older model, red Chevrolet pick-up truck, driving west on Clayton Road before the robbery and speeding east on Clayton Road after the robbery towards Highway 40/64. The truck had significant front-end damage and a black tool box in the bed of the truck.

9. On April 18, 2019, a bank robbery occurred at the Bank of America, 4189 Veteran's Memorial Parkway, St. Peters, MO, in the Eastern District of Missouri. An unknown male entered the bank wearing a blue mask, dark hooded sweatshirt, dark pants and blue latex gloves and announced the robbery. The unknown male was holding a dark colored semi-automatic firearm which he pointed at employee(s). The victim teller proceeded to give the unknown male approximately \$6,400.00 in US Currency belonging to Bank of America. Included in the funds was a tracking device. The unknown male exited the bank and traveled away from the location. Witness(es) noted two vehicles leaving the bank parking lot shortly

after the unknown male fled the area. One of the vehicles was a white/light colored sedan and the other was an older maroon Chevrolet pickup. Responding law enforcement authorities were directed to the area of 1411 Park Court, St. Charles, MO, based on the tracking device deployed by the bank. At that location, law enforcement authorities located a maroon 1995 Chevrolet S-10 with Missouri License Plate – 6ABK93. A witness to the robbery was conveyed to the location of the vehicle and identified it as the vehicle he witnessed leaving the bank parking lot after the robbery. Law enforcement authorities were able to confirm that the tracking device deployed by the bank was located inside the vehicle using a handheld electronic tracking system device. Visible through the window was a black sweatshirt, blue latex gloves, a black handgun, and US Currency. The Missouri License Plate is registered to a maroon 1995 Chevrolet S-10, owned by **Ricardo RUSAN**, 985 Grenoble Lane, Florissant, MO 63033.

10. On April 18, 2019, law enforcement obtained and executed a search warrant for the vehicle. The search warrant was from the State of Missouri, County of St. Charles. Items located inside the vehicle included: clothes consistent with those used by the unknown male bank robber, blue latex gloves, US Currency in the approximate amount stolen during the bank robbery, a blue mask consistent with the mask used during the bank robbery, paperwork in the name of **Ricardo RUSAN**, two cellular telephones, and a black pellet type handgun.

11. On June 11, 2019, the St. Charles County Police Department, Criminalistics Laboratory issued a report detailing a CODIS Notification Match on a DNA profile found on the blue plastic mask found in **RUSAN**'s vehicle after the April 18, 2019 robbery of the Bank of America, 4189 Veterans Memorial Parkway, St. Peters, MO. The DNA profile on the mask matched previously obtained DNA from **RUSAN**.

12. On June 20, 2019, **RUSAN** was Indicted for Bank Robbery and an Arrest Warrant was issued from the United States District Court for the Eastern District of Missouri for Bank Robbery under No: 4:19CR00469 HEA/SPM.

13. On July 18, 2019, an agent with the FBI interviewed K.S. **RUSAN**. K.S. indicated that they were “friends” with **RUSAN** on Facebook and that **RUSAN**’s Facebook profile was under “Ricardo Rusan-el.” During the interview, K.S. opened the Facebook profile, “Ricardo Rusan-el”, **the target account**, and indicated that the last activity they could see was on or about June 20, 2019.

14. On July 18, 2019, an agent with the FBI viewed **the target account** Facebook account “Ricardo Rusan-el” and located several photographs of an individual, based on a comparison with a driver’s license photograph, believed to be **RUSAN**.

#### **BACKGROUND INFORMATION ABOUT THE PROVIDER**

15. From my consultations with personnel familiar with stored electronic communications, remote computing services and social media network sites, and my own training, experience and knowledge, I am aware that:

16. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

17. An “Internet Protocol” (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aids in identifying the location of digital devices that are connected to

the Internet so that they can be differentiated from other devices. As a mailing address allows a sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

18. “Internet Service Provider” (ISP) is an entity that provides access to the Internet to its subscribers.

19. The term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.

20. Facebook is a business and company that operates as a remote computing service, a provider of electronic communications services through ISPs. Facebook owns and operates a free-access social networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Services offered by Facebook are diverse and include the operation of a free, internet-based social media and networking site. Users create their own profile pages, which can include personal information, lists of personal interests, photographs, videos, and messages. Once an account is created a Facebook user can invite and ‘add’ friends to their Facebook account, and links to pages within and outside the Facebook environment. Facebook also permits users to send and receive private messages (the functional equivalent of e-mails) with other Facebook users, and to restrict the disclosure of certain information (profile information, photos, messages, videos and other content) exclusively to the selected groups of individuals such as Facebook ‘friends’ of their choosing.

21. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact e-mail addresses, Facebook passwords, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook asks users to provide basic identity and contact information to Facebook, either during the registration process or thereafter. Facebook also assigns a user identification number to each account. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook. Each user profile page includes a list of that user's 'friends,' along with links to the friends' profiles pages. Facebook users can adjust the privacy settings for their profile so that their profile information is visible only to their Facebook 'friends,' rather than to the public (which is the default setting).

22. For each user, Facebook retains information about the date and time at which the user's profile was created, the date and time at which the account was created, and the IP address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Facebook account. For a given user, Facebook retains the basic identity information entered by the user, all data displayed on the user's profile, and all stored files (such as images and videos) contained in the user's account as long as the user has not edited the data or removed

the files from the profile. When a given Facebook account is deleted, Facebook retains certain information relating to that account for some period of time, including user identity information, IP logs, and other data. Even if a given user deletes data, Facebook stores such data for extended periods of time on Facebook's servers. Facebook typically retains additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number).

23. Facebook regularly maintains information about the precise location of a device used to access a particular account, either through cellular towers, built-in GPS, or wireless access points, or internet service provider addresses. This information is used to provide tailored advertisements and other services to users. In the case of a mobile telephone, depending on a user's settings, Facebook can continue to obtain precise location information.<sup>1</sup>

24. As explained herein, location information stored in connection with a Facebook account may provide crucial information leading to the location of an individual as well as the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling law enforcement to locate said individual for apprehension purposes and/or to establish and prove each element or alternatively, to exclude the innocent from further suspicion.

25. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends'

---

<sup>1</sup>[https://www.facebook.com/location\\_history/info/](https://www.facebook.com/location_history/info/)

Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

26. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information in the user's account available only to himself or herself, to other specified Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s).

27. Facebook also keeps internet protocol (IP) logs for each user. These logs contain information about the user's log-ins to Facebook, including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile. Facebook retains IP log information about each account access for at least ninety days; however, in some instances the data may be retained for longer or shorter periods of time.

28. Facebook users can exchange private mail messages with other users via Facebook. A given private message typically includes the Facebook user name of the sender and the recipient of the message, a subject line, the actual content of the message, and a date stamp reflecting when the message was sent. Private messages are sent to the recipient's Facebook

inbox and remain available until the user removes them. A user's sent messages are stored in a 'sent box' for that user on Facebook.

29. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

30. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and creator of the group. Facebook also assigns a group identification number to each group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and administrator, as well as the current status of the group profile page.

31. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

32. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a

personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

33. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user’s access or use of that application may appear on the user’s profile page.

34. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post “status” updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming “events,” such as social occasions, by listing the event’s time, location, host, and guest list. A particular user’s profile page also includes a “Wall,” which is a space where the user and his or her “Friends” can post messages, attachments, and links that will typically be visible to anyone who can view the user’s profile.

35. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to “tag” (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook’s purposes, a user’s “Photoprint” includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

36. Facebook users can add a variety of information to their profiles, including photographs, videos, music and other audio files, lists of personal interests and preferences,

journals or web logs ('blogs'), bulletins, news feeds, links to other locations on the Internet, which typically contain personal information about the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles. Facebook allows users to edit or delete comments on their own profile pages, and users can adjust their profile settings to allow them to pre-approve comments on their own profile pages.

37. Messages, photos, audio videos, and other records stored on Facebook server by a subscriber may not necessarily be located in the subscriber's home/work computer. The subscriber or user may store data on Facebook servers for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer at his/her residence or employment. A search of the files in the computer at the subscriber's residence or place of employment will not necessarily uncover the files that the subscriber has stored on the Facebook server. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

38. It is common for individuals involved in criminal offenses to communicate with one another through Facebook and other online social media e-mail methods. Such communication includes discussions concerning planning, operations, intelligence gathering and dissemination, the transfer of critical information, the staging of videos, the identification and photos of money and contraband gained from criminal activities, and the identification of other associates and co-conspirators.

39. From my knowledge, training and experience, as well as discussions I have had with other agents and personnel familiar with computer-related investigations, I know that it is

common for individuals engaged in the criminal activities described herein to use websites, social networking sites, and other internet-based applications to communicate with one another and facilitate their criminal activities. Such communications and the facilitation of criminal activities include the use of these applications and electronic and stored data that would identify and describe: (a) other co-conspirators, aiders, and abettors who are participating in the illegal activities as well as the nature and scope of the illegal activities; (b) identify dates and locations where illegal activity has taken place or may take place in the future; (c) financial transactions and monetary transfers used to facilitate and continue criminal activities as well as the existence and location of records, bank accounts, and businesses pertaining to those activities; (d) sales and purchases of equipment, materials, and goods used to aid the co-conspirators in their endeavors as well as the location and use of assets accumulated; (e) travel, safe-houses, and locations where goods, materials and personnel stay or are kept; and, (f) the existence of other communication facilities, including telephones, computers, e-mail and other electronic accounts used to by co-conspirators to communicate.

40. By its very nature, websites, social networking accounts, and internet-based applications described herein are kept and stored in computers and electronic-memory devices by the host companies, in addition to or in lieu of hard-copy versions of this data. Because such evidence is stored electronically, the data and evidence of the crimes described herein may be stored and be present for long periods of time.

41. In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support

services, as well as records of any actions taken by the provider or user as a result of the communications.

42. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user’s IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used. For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Facebook “friends” to locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner’s state of mind as it

relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

43. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers, location information, and their use of Facebook, such as account access information, transaction information, and other account information.

44. As described earlier in this affidavit, it is common for individuals involved in these activities and criminal offenses to communicate with one another through online methods such as Facebook and other online sources. Such communication includes discussions concerning planning, operations, the transfer of information, and the identification of other associates and co-conspirators. As is apparent this enables individuals to share photographs, videos, documents, files, and information. Online social media sites such as Facebook allow individuals to communicate and disseminate information to numerous individuals at one time, such as "Friends" and "Groups." Postings and sharing information can quickly reach large audiences in an efficient manner. Facebook in particular also allows users to have private discussions, messages, and communications that may otherwise not be possible.

45. Therefore, the computers of Facebook are likely to contain all the material described above, including information concerning the location of the device(s) being used to access the Target Account.

**OTHER CONSIDERATIONS: NOTIFICATION AND TIME OF EXECUTION**

46. Based on my training and experience in locating and apprehending potentially violent fugitives, the data being sought by this warrant will assist in locating **RUSAN**. Because successful apprehensions, particularly of violent fugitives, often rely on the element of surprise and on approaching the fugitive at a time most advantageous to law enforcement officers in consideration of the safety of all parties involved, it is often necessary to attempt an arrest during nighttime or the early morning hours. Further, apprehension plans often change at the last minute based on unexpected movements or other behavior of the target. Therefore, it is not possible to predict in advance when the location information would need to be accessed. Further, this investigation concerns the search for a person who is the subject of an outstanding arrest warrant, which itself may be served at any time of day or night. As such, I request that the Court's warrant authorize the execution of said warrant and the obtaining of the requested information at any time of the day or night.

47. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until for a period of one year after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Account would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2).

Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

### **CONCLUSION AND REQUEST FOR SEALING**

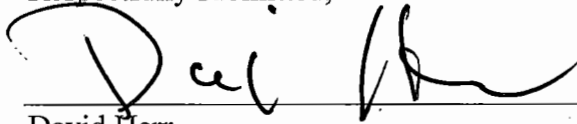
48. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703(c).

49. I further request that the Court direct Facebook to disclose to the government any information described in Attachment B that is within the possession, custody, or control of Facebook. I also request that the Court direct Facebook to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with Facebook's services. The government shall reasonably compensate Facebook for reasonable expenses incurred in furnishing such facilities or assistance.

50. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Based upon my training and experience, I am informed that criminals actively search online for criminal affidavits and search warrants via the internet, and disseminate them to other others as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation

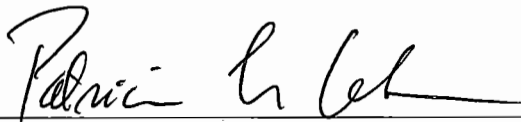
and may severely jeopardize its effectiveness. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "David Herr", written over a horizontal line.

David Herr  
Special Agent  
Federal Bureau of Investigation (FBI)

Subscribed and sworn to before me on this 24 day of July, 2019

A handwritten signature in black ink, appearing to read "Patricia L. Cohen", written over a horizontal line.

HONORABLE PATRICIA L. COHEN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

1. The account associated with user ID <https://www.facebook.com/ricardo.rusanel> (the “Target Account”), whose service provider is **Facebook, Inc.**, a company headquartered at **1601 Willow Road, Menlo Park, California.**
2. Records and information associated with the Target Account that is within the possession, custody, or control of **Facebook, Inc.**

## **ATTACHMENT B**

### **Particular Things to be Seized**

#### **I. Information to be Disclosed by the Provider**

All information about the location of the Target Account described in Attachment A for a period of thirty (30) days prior, continuing for a period of thirty (30) days into the future, during all times of day and night. "Information about the location of the Target Account" includes, but is not limited to any data collected by Facebook, Inc.'s location services via the user's mobile phone or other device, on a real-time or near-real time basis. Facebook is required to provide any such data they collect, regardless of the time of day. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

#### **II. Information to Be Seized by the Government**

All information described above in Section I that will assist in arresting **Ricardo RUSAN**, who was charged with violating **Title 18, United States Code, Section 2113** on **June 20, 2019**, is the subject of an arrest warrant issued on **June 20, 2019**, and is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

**FACEBOOK, INC.** is hereby ordered to disclose the above information to the government within 14 days of the date of this warrant.